대한민국특허청
KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : 특허출원 2004년 제 0067733 호
Application Number 10-2004-0067733

출 원 년 월 일 : 2004년 08월 27일
Date of Application AUG 27, 2004

출 원 인 : 한국전자통신연구원 외 5명
Applicant(s) Electronics and Telecommunications Research Institute, et al.

2004 년 11 월 15 일

특 허 청
COMMISSIONER

【서지사항】

【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【출원일자】	2004.08.27
【발명의 명칭】	무선 휴대 인터넷 시스템에서의 가입자 단말 인증 방법 및 그 프로토콜 구성 방법, 그리고 그 장치
【발명의 영문명칭】	METHOD FOR AUTHENTICATING SUBSCRIBER STATION IN WIRELESS PORTABLE INTERNET SYSTEM AND PROTOCOL CONFIGURATION METHOD THEREOF, AND APPARATUS THEREOF
【출원인】	
【명칭】	한국전자통신연구원
【출원인코드】	3-1998-007763-8
【출원인】	
【명칭】	삼성전자 주식회사
【출원인코드】	1-1998-104271-3
【출원인】	
【명칭】	주식회사 케이티
【출원인코드】	2-1998-005456-3
【출원인】	
【명칭】	주식회사 케이티프리텔
【출원인코드】	1-1998-098986-8
【출원인】	
【명칭】	에스케이텔레콤 주식회사
【출원인코드】	1-1998-004296-6
【출원인】	
【명칭】	하나로통신 주식회사
【출원인코드】	1-1998-112749-2
【대리인】	
【명칭】	유미특허법인
【대리인코드】	9-2001-100003-6
【지정된변리사】	이원일

【포괄위임등록번호】 2001-038431-4
【포괄위임등록번호】 2002-036528-9
【포괄위임등록번호】 2003-082444-7
【포괄위임등록번호】 2002-031524-6
【포괄위임등록번호】 2002-062290-2
【포괄위임등록번호】 2004-014783-3
발명자】
【성명의 국문표기】 박애순
【성명의 영문표기】 PARK,AE SOON
【주민등록번호】 640920-2401130
【우편번호】 305-755
【주소】 대전광역시 유성구 어은동 한빛아파트 138동 301호
【국적】 KR
발명자】
【성명의 국문표기】 조석헌
【성명의 영문표기】 CHO,SEOK HEON
【주민등록번호】 770127-1543416
【우편번호】 570-976
【주소】 전라북도 익산시 신동 775-21번지
【국적】 KR
발명자】
【성명의 국문표기】 임선화
【성명의 영문표기】 LIM,SUN HWA
【주민등록번호】 700409-2095814
【우편번호】 302-793
【주소】 대전광역시 서구 월평동 주공아파트 207동 1004호
【국적】 KR
발명자】
【성명의 국문표기】 김영진
【성명의 영문표기】 KIM,YEONG JIN
【주민등록번호】 570808-1550312

【우편번호】 302-791
【주소】 대전광역시 서구 월평동 누리아파트 107동 1401호
【국적】 KR
명자】
【성명의 국문표기】 안지환
【성명의 영문표기】 AHN,JEE HWAN
【주민등록번호】 560617-1460611
【우편번호】 305-804
【주소】 대전광역시 유성구 신성동 149-7번지
【국적】 KR
선권주장】
【출원국명】 KR
【출원종류】 특허
【출원번호】 10-2003-0076554
【출원일자】 2003.10.31
【증명서류】 첨부
사청구】 청구
지】 특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 출원심사 를 청구합니다. 대리인
유미특허법인 (인)
수료】
【기본출원료】 0 면 38,000 원
【가산출원료】 51 면 0 원
【우선권주장료】 1 건 20,000 원
【심사청구료】 24 항 877,000 원
【합계】 935,000 원
부서류】 1. 우선권증명서류 원문[특허청기제출]_1통

【요약서】

【요약】

본 발명은 무선 휴대 인터넷 시스템에서의 가입자 단말 인증 방법 및 그 프로토 구성 방법, 그리고 그 장치에 관한 것이다. 본 발명의 가입자 단말 인증 방법은 입자 단말과 기지국 간의 인증 모드 협상이 먼저 이루어지고, 이러한 인증 모드 협에 따라 기지국에 의해 인증 모드가 설정된다. 설정될 수 있는 인증 모드에는 EE 802.16 프라이버시 표준 프로토콜 기반의 인증 모드와 상위 계층의 표준화된 인 프로토콜 기반의 인증 모드가 있다. IEEE 802.16 프라이버시 표준 프로토콜 기반 인증 모드인 경우에는 기지국에서 인증이 이루어지고, 상위 계층의 표준화된 인증 로토콜 기반의 인증 모드인 경우에는 기지국과 인증 서버 간의 다이아메터 프로토 을 이용한 메시지의 전송을 통해 인증이 이루어진다. 본 발명에 따르면, IEEE 2.16에서 지원하는 가입자 단말의 인증 기능에 이동 가입자 단말에 대한 지원이 가 해진다. 또한, 서로 다른 사업자 망들간에 연동 또는 동일 사업자이지만 서로 다 망으로 구성된 경우에 대해서도 이들 망간의 연동 지원이 가능해진다.

【대표도】

도 5

【색인어】

선 휴대 인터넷, 가입자 인증, 상위 계층 프로토콜, EAP, MAC 메시지, PKM, privacy, EE 802.16

【명세서】

【발명의 명칭】

무선 휴대 인터넷 시스템에서의 가입자 단말 인증 방법 및 그 프로토콜 구성
법, 그리고 그 장치 (METHOD FOR AUTHENTICATING SUBSCRIBER STATION IN WIRELESS
PORTABLE INTERNET SYSTEM AND PROTOCOL CONFIGURATION METHOD THEREOF, AND APPARATUS
THEREOF)

【도면의 간단한 설명】

도 1은 본 발명의 실시예에 따른 무선 휴대 인터넷의 개요를 도시한 개
략도이다.

도 2는 도 1에 도시된 무선 휴대 인터넷 시스템의 계층 구조를 도시한 계층도이
다.

도 3은 도 1에 도시된 무선 휴대 인터넷 시스템에서 기지국과 가입자 단말의 연
결 구조를 도시한 개략도이다.

도 4는 본 발명의 실시예에 따른 무선 휴대 인터넷 시스템에서의 연결 설정을
위한 흐름도이다.

도 5는 도 4에 도시된 기본 기능 협상 과정 및 가입자 단말 인증 과정을 수행하
기 위해 가입자 단말과 기지국 간의 MAC 연결 절차를 나타내는 흐름도이다.

도 6은 도 5에 도시된 기본 기능 협상 과정에서 사용되는 기본 기능 협상 요구
메시지(SBC-REQ)의 포맷을 나타낸 도면이다.

도 7은 본 발명의 실시예에 따른 무선 휴대 인터넷 시스템에서의 가입자 단말 증 방법에서 EAP 기반으로 가입자 단말을 인증하기 위한 MAC 흐름도이다.

도 8은 본 발명의 실시예에 따른 무선 휴대 인터넷 시스템에서의 가입자 단말 증 방법에서 사용되는 MAC 메시지 중 PKM 메시지의 타입을 나타낸 도면이다.

도 9는 도 8에 도시된 PKM 메시지 중에서 EAP 기반의 가입자 인증을 위한 메시의 구성요소를 나타낸 도면이다.

도 10은 도 6에 도시된 기본 기능 협상 요구 메시지(SBC-REQ)의 파라미터 중 thorization Policy Support 파라미터의 속성을 나타낸 도면이다.

도 11은 본 발명의 실시예에 따른 무선 휴대 인터넷 시스템에서의 가입자 단말 증 장치의 블록도이다.

도 12는 도 11에 도시된 가입자 단말의 인증 요청부의 상세 블록도이다.

도 13은 도 11에 도시된 기지국의 인증 처리부의 상세 블록도이다.

도 14는 도 11에 도시된 AAA 서버의 인증 처리부의 상세 블록도이다.

발명의 상세한 설명

발명의 목적

발명이 속하는 기술분야 및 그 분야의 종래기술

본 발명은 무선 휴대 인터넷 시스템에서의 가입자 단말 인증 방법에 관한 것으. 보다 구체적으로 무선 휴대 인터넷 시스템에서 이동 가입자 및 망간 연동시의 가 자 인증을 위해 상위 계층의 표준화된 프로토콜을 수용하는 무선 휴대 인터넷 시스

에서의 가입자 단말 인증 방법 및 그 프로토콜 구성 방법, 그리고 그 장치에 관한 이다.

무선 휴대 인터넷은 종래의 무선 LAN과 같이 고정된 액세스 포인트(Access int:AP)를 이용하는 근거리 데이터 통신 방식에 이동성(mobility)을 더 지원하는 세대 통신 방식이다. 이러한 무선 휴대 인터넷은 다양한 표준들이 제안되고 있으, 현재 IEEE 802.16을 중심으로 휴대 인터넷의 국제 표준화가 진행되고 있다.

이러한 IEEE 802.16에서 정의하는 인증(Authentication and authorization) 규은 무선 네트워크로 구성된 광대역 네트워크를 대상으로 단말에 대한 인증 기능을 격화하고 있다. 특히, IEEE 802.16의 프라이버시(privacy) 계층으로 규격화하여 의하고 있는 가입자 단말(Subscriber Station, 이하 "SS"라고 함)에 대한 인증 기은 주로 고정망에서의 사용자를 대상으로 하기 때문에 현재 이동 서비스의 추세인 말 또는 가입자의 이동성 지원에 적합하지 않다. 즉, 고정망을 기반으로 SS의 인을 위한 메시지 및 절차가 기술되어 있는 기지국(Base Station, 이하 "BS"라고 함) 서의 구체적 기능들이 명시되어 있지 않아서, 이동서비스를 위해서는 추가적으로 의 기능 요구가 이루어져야 한다. 이러한 추가적인 기능 요구는 개략적으로 BS에 현재 서비스를 받는 모든 가입자에 대한 프로파일을 갖고 있거나, 그렇지 않은 경 CA 인터페이스를 위한 API 또는 인증 서버와의 인터페이스를 위한 인증 클라이언 수용등의 기능을 요구한다.

또한, 종래 고정망에서의 가입자 단말에 대한 인증은 디지털 인증서 반이므로, 인증 서버에 접속하여 사용자 인증을 받는 경우 반드시 인증서 기반의 증을 수행하는 서버로 제한되며, 기존 규격의 경우 SS와 BS사이의 보안을 위한 키

배를 BS에서 하도록 정의되어 있어, BS 자체에 대한 보안에도 또 다른 향상된 기능 필요하다는 문제점이 있다.

발명이 이루고자 하는 기술적 과제】

따라서, 본 발명의 목적은 상기한 문제점을 해결하고자 하는 것으로, 가입자 단에 대한 인증시에 이동 가입자 단말이나 망간의 연동에 따른 가입자 단말에 대해 준화된 상위 계층의 프로토콜을 수용한 인증이 가능하도록 한 무선 휴대 인터넷 시템에서의 가입자 단말 인증 방법 및 그 프로토콜 구성 방법, 그리고 그 장치를 제하는 것이다.

발명의 구성 및 작용】

상기 과제를 달성하기 위한 본 발명의 하나의 특징에 따른 무선 휴대 인터넷 시템에서의 가입자 단말 인증 요청 방법은,

무선 휴대 인터넷 시스템에서 기지국에 무선 연결된 가입자 단말이 기지국으로 증을 요청하는 방법으로서,

a) 인증 모드 설정을 위해 기본 능력 협상 메시지를 상기 기지국으로 송신하는 계: b) 상기 기지국에서 송신된 상기 기본 능력 협상 메시지에 대한 응답 메시지를 신하여 인증 모드를 설정하는 단계: 및 c) 상기 설정된 인증 모드에 대응되는 가입 인증 요청 메시지를 상기 기지국으로 송신하여 상기 가입자 단말에 대한 인증을 청하는 단계를 포함한다.

여기서, 상기 a) 단계에서, 상기 기본 능력 협상 메시지에는 인증 모드 설정이 능한 파라미터가 포함된 것을 특징으로 한다.

또한, 상기 b) 단계에서, 상기 인증 모드는 IEEE 802.16 프라이버시 표준 프로토콜에 기반한 인증 모드와 상위 계층의 표준화된 인증 프로토콜에 기반한 인증 모드 중 어느 하나인 것을 특징으로 한다.

또한, 상기 b) 단계에서 상기 인증 모드가 상위 계층의 표준화된 인증 프로토콜에 기반한 인증 모드로 설정된 경우, 상기 c) 단계에서, 상기 기지국에 접속되어 상기 가입자에 대한 인증을 수행하는 인증 서버(AAA:Authentication Authorization and Accounting 서버)에 의한 가입자 인증을 요청하는 가입자 인증 요청 메시지를 상기 기지국을 통해 상기 인증 서버로 송신하는 것을 특징으로 한다.

본 발명의 다른 특징에 따른 무선 휴대 인터넷 시스템에서의 가입자 단말 인증 방법은,

무선 휴대 인터넷 시스템에서 기지국에 무선 연결된 가입자 단말에 대한 인증을 수행하는 방법으로서,

a) 상기 가입자 단말로부터 수신되는 인증 모드 설정을 위한 기본 능력 협상 메시지에 따라 인증 모드를 설정한 응답 메시지를 상기 가입자 단말로 송신하는 단계; 상기 가입자 단말로부터 가입자 인증을 요청하는 메시지를 수신하여 직접 인증을 수행하거나 또는 상기 기지국에 접속되어 상기 가입자에 대한 인증을 수행하는 인증 서버(AAA:Authentication Authorization and Accounting 서버)에게 가입자 인증을 요청하는 단계; 및 c) 상기 인증 결과를 나타내는 응답 메시지를 상기 가입자 단말로 송신하는 단계를 포함한다.

본 발명의 또 다른 특징에 따른 무선 휴대 인터넷 시스템에서의 가입자 단말 인 프로토콜 구성 방법은,

무선 휴대 인터넷 시스템에서 가입자 단말과 기지국 간에 가입자 단말에 대한 증을 수행하는 프로토콜을 구성하는 방법으로서,

a) 상기 가입자 단말과 기지국 간에 인증 모드 설정을 위한 기본 능력 협상 메지를 MAC 메시지를 이용하여 송수신하는 단계; 및 b) 상기 가입자 단말과 기지국에 상기 a) 단계에서 설정된 인증 모드에 따른 가입자 인증 메시지를 MAC 메시지를 용하여 송수신하는 단계를 포함한다.

여기서, 상기 기본 능력 협상 메시지는 IEEE 802.16 프라이버시 표준 프로토콜 MAC 메시지 중 하나인 SBC-REQ 및 SBC-RSP 메시지에 인증 모드 설정이 가능한 파미터가 포함된 메시지를 이용하여 전송되는 것을 특징으로 한다.

또한, 상기 b) 단계에서, 상기 가입자 인증 메시지는 IEEE 802.16 표준 프로토의 MAC 메시지 중 하나인 PKM-REQ 및 PKM-RSP 메시지 또는 상기 PKM-REQ 및 M-RSP 메시지에 상위 계층의 표준화된 프로토콜에 따른 인증을 수행하기 위한 메시를 이용하여 전송되는 것을 특징으로 한다.

본 발명의 또 다른 특징에 따른 가입자 단말은,

무선 휴대 인터넷 시스템에서 기지국에게 인증을 요청하는 가입자 단말로서,

상기 기지국에게 가입자 단말에 대해 수행될 인증 모드 설정을 요청하고, 상기 지국에 의해 설정된 인증 모드에 따른 가입자 단말에 대한 인증을 상기 기지국으로 청하는 단말기 제어 장치; 상기 단말기 제어 장치로 입출력되는 신호에 대한 변복

및 채널 부호화를 수행하는 디지털 신호 송수신 장치; 및 상기 디지털 신호 송수신 장치와 상기 기지국 간의 아날로그 무선 신호 전송을 중개하는 아날로그 신호 송수신 장치를 포함한다.

본 발명의 또 다른 특징에 따른 기지국 장치는,

무선 휴대 인터넷 시스템에서 가입자 단말에 대한 인증을 수행하는 기지국 장치서,

상기 가입자 단말로부터의 인증 요청에 따라 인증 모드를 설정하고, 상기 설정된 인증 모드에 따른 인증을 수행하는 기지국 제어 장치; 상기 기지국 제어 장치로 출력되는 신호에 대한 변복조 및 채널 부호화를 수행하는 디지털 신호 송수신 장치; 및 상기 디지털 신호 송수신 장치와 상기 가입자 단말 간의 아날로그 무선 신호 전송을 중개하는 아날로그 신호 송수신 장치를 포함한다.

아래에서는 첨부한 도면을 참고로 하여 본 발명의 실시예에 대하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였다. 명세서 전체를 통하여 유사한 부분에 대해서는 동일한 도면 부호를 붙였다.

이하, 첨부된 도면을 참조하여 본 발명의 실시예에 따른 무선 휴대 인터넷 시스템에서의 가입자 단말 인증 방법에 대해서 상세하게 설명한다.

도 1은 본 발명의 실시예에 따른 무선 휴대 인터넷의 개요를 도시한 략도이다.

도 1에 도시된 바와 같이, 무선 휴대 인터넷 시스템은 기본적으로 가입자 단말 S, 10), 가입자 단말(10)과 무선 통신을 수행하는 기지국(BS, 20, 21), 기지국(20,)에 접속되어 게이트웨이를 통해 접속된 라우터(30, 31) 및 라우터(30, 31)에 접속어 가입자 단말(20, 21)에 대한 인증을 수행하는 인증 서버(AAA:Authentication thorization and Accounting) 서버(40)를 포함한다.

종래의 IEEE 802.11과 같은 무선 LAN 방식은 고정된 액세스 포인트를 중심으로 거리내에서 무선 통신이 가능한 데이터 통신 방식을 제공하고 있으나, 이는 가입자 말의 이동성을 제공하는 것이 아니고, 단지 유선이 아닌 무선으로 근거리 데이터 신을 지원한다는 한계를 가지고 있었다.

한편, IEEE 802.16 그룹 등에서 추진중인 무선 휴대 인터넷 시스템은 도 1에 도 된 가입자 단말(10)이 기지국(20)이 관장하는 셀에서 기지국(21)이 관장하는 셀로 등하는 경우에도 그 이동성을 보장하여 끊기지 않는 데이터 통신 서비스를 제공하 된다.

이러한 IEEE 802.16은 기본적으로 도시권 통신망(Metropolitan Area Network, N)을 지원하는 규격으로서, 구내 정보 통신망(LAN)과 광역 통신망(WAN)의 중간 정의 지역을 망라하는 정보 통신망을 의미한다.

따라서, 무선 휴대 인터넷 시스템은 이동통신 서비스와 같이 가입자 단말(10)의 핸드오버를 지원하며, 가입자 단말의 이동에 따라 동적인 IP 어드레스 할당을 수행하게 된다.

여기서, 무선 휴대 인터넷 가입자 단말(10)과 기지국(20, 21)은 직교 주파수 분할 다중화(Orthogonal Frequency Division Multiple Access: 이하 OFDMA라고 함)방식으로 통신을 수행한다. OFDMA 방식은 복수의 직교주파수의 부반송파(sub carrier)를 복수의 서브 채널로 이용하는 주파수 분할 방식과, 시분할 방식(TDM) 방식을 결합한 다중화 방식이다. 이러한 OFDMA 방식은 본질적으로 다중 경로(multi path)에서 발생하는 페이딩(fading)에 강하며, 데이터 전송률이 높다.

한편, 가입자 단말(10)과 기지국(20, 21)은 통신을 시작하면서 가입자 단말(10)에 대한 인증을 위한 인증 모드를 협상하고, 협상 결과에 따라 선택된 방식의 인증 절차를 수행한다. 즉, 가입자 단말(10)과 기지국(20, 21)은 협상을 통해 종래의 IEEE 802.16 프라이버시 규격에 따른 디지털 인증서 기반의 인증 모드와 상위 계층의 표준화된 인증 프로토콜 기반의 인증 모드 중 하나를 선택하고, 선택된 인증 모드에 따라 가입자 단말(10)에 대한 인증 절차를 수행한다.

이 때, 상위 계층의 표준화된 인증 프로토콜은 EAP(Extensible Authentication Protocol) 프레임워크(framework)인 EAP-TLS(Transport Layer Security) 또는 EAP-TTLS(Tunneled TLS) 중 어느 하나일 수 있다.

한편, 가입자 단말(10)과 기지국(20, 21) 간의 인증 모드 협상에 따라 상위 계층의 표준화된 인증 프로토콜 기반의 인증 모드가 선택되면, 가입자 단말(10)과 기지국(20)은 상위 계층의 표준화된 인증 프로토콜 기반의 인증 절차를 수행하기 위한 준

를 한 후, 가입자 단말(10)은 인증을 위한 메시지를 생성하여 기지국(20)으로 전달고, 기지국(20)은 해당 인증 서버인 AAA 서버(40)와의 상호 작용을 통해 가입자 단(10)에 대한 인증을 수행한다.

도 2는 도 1에 도시된 무선 휴대 인터넷 시스템의 계층 구조를 도시한 계층도이

.

도 2에 도시된 바와 같이, IEEE 802.16의 무선 휴대 인터넷 시스템의 계층 구조 크게 물리 계층(Physical Layer, L10)과 매체 접근 제어(Media Access Control: 하 "MAC" 이라고 함) 계층(L21, L22, L23)으로 구분된다.

물리 계층(L10)은 변복조 및 코딩 등 통상의 물리 계층에서 수행하는 무선 통신 능을 담당하고 있다.

한편, 무선 휴대 인터넷 시스템은 유선 인터넷 시스템과 같이 그 기능별로 세분된 계층을 가지지 않고 하나의 MAC 계층에서 다양한 기능을 담당하게 된다.

그 기능별로 서브 계층을 살펴보면, MAC 계층은 프라이버시 서브계층(Privacy blayer, L21), MAC 공통부 서브계층(MAC Common Part Sublayer, L22), 서비스 특정 합 서브계층(Service Specific Convergence Sublayer, L23)을 포함한다.

프라이버시 서브계층(L21)은 장치 인증 및 보안키 교환, 암호화 기능을 수행한 . 프라이버시 서브계층(L21)에서 장치에 대한 인증만이 수행되고, 사용자 인증은 C의 상위 계층(도시 생략)에서 수행된다.

MAC 공통부 서브계층(L22)은 MAC 계층의 핵심적인 부분으로서 시스템 액세스, 역폭 할당, 트래픽 연결(Traffic Connection) 설정 및 유지, QoS 관리에 관한 기능 담당한다.

서비스 특정 집합 서브계층(L23)은 연속적인 데이터 통신에 있어서, 페이로드 더 서프레션(suppression) 및 QoS 맵핑 기능을 담당한다.

도 3은 도 1에 도시된 무선 휴대 인터넷 시스템에서 기지국(20, 21)과 가입자 말(10)의 연결구조를 도시한 개략도이다.

도 3에 도시된 바와 같이, 가입자 단말(10)의 MAC 계층과 기지국(20, 21)의 MAC 층은 트래픽 연결(Traffic Connection, C1)이라는 개념이 존재한다.

여기서, "트래픽 연결(C1)"이란 용어는 물리적 연결관계가 아니라 논리적 연결 계를 의미하는 것으로서, 하나의 서비스 플로우에 대하여 트래픽을 전송하기 위해 입자 단말(10)과 기지국(20, 21)의 MAC 동위계층(peer)들 사이의 맵핑 관계로 정의다.

따라서, 상기 트래픽 연결(C1) 상에서 정의되는 파라미터 또는 메시지는 MAC 등 계층간의 기능을 정의한 것이며, 실제로는 그 파라미터 또는 메시지가 가공되어 레임화되어 물리 계층을 거쳐 전송되고, 상기 프레임을 분석하여 MAC 계층에서 그 라미터 또는 메시지에 대응하는 기능을 수행하게 되는 것이다.

그 밖에도 MAC 메시지는 각종 동작에 대한 요청(REQ), 응답(RSP), 확인(ACK)기을 수행하는 다양한 메시지를 포함한다.

도 4는 본 발명의 실시예에 따른 무선 휴대 인터넷 시스템에서의 연결 설정을 한 흐름도이다.

도 4를 참조하면, 가입자 단말(10)이 기지국(20)에 진입하면(S10), 우선 기지국(0)은 가입자 단말(10)과 하향링크 동기를 설정한다(S20).

이와 같이, 기지국(20)에서 하향링크 동기가 설정되면, 가입자 단말(10)은 상향크 파라미터를 획득하게 된다(S30). 예를 들어, 상기 파라미터는 물리 계층의 특(예를 들어, 신호대 잡음비)에 따른 채널 디스크립터 메시지를 포함할 수 있다.

그 후, 가입자 단말(10)과 기지국(20)은 레인징(Ranging) 절차를 수행한다(40). 여기서 레인징은 가입자 단말(10)과 기지국(20) 간의 타이밍, 전력, 주파수 보를 정정하여 일치시키는 것으로서, 최초에 초기 레인징(initial ranging)을 수행고, 이후 주기적으로 주기적 레인징(periodic ranging)을 수행하게 된다.

이러한 레인징 절차(S40)가 완료되면, 가입자 단말(10)과 기지국(20) 간의 연결 설정을 위한 단말 기본 기능에 관한 협상이 수행된다(S50). 이러한 과정(S50)에서 입자 단말(10)과 기지국(20, 21)은 협상을 통해 종래의 IEEE 802.16 프라이버시 규에 따른 디지털 인증서 기반의 인증 모드와 상위 계층의 표준화된 인증 프로토콜, 를 들어 EAP-TLS, EAP-TTLS 등의 프로토콜 기반의 인증 모드 중 하나를 선택할 수다.

이와 같이, 인증 모드를 포함한 여러 기본 기능에 대한 협상이 완료되면, 기지(20)은 상기 단계(S50)에서 선택된 인증 모드에 따라 가입자 단말(10)에 대한 인증 수행한다(S60).

가입자 단말(10)의 인증이 완료되어 무선 휴대 인터넷의 사용 권한이 확인되면, 지국(20)은 가입자 단말(10)의 장치 어드레스를 등록한다(S70). 그 후, 기지국 0)은 DHCP 서버 또는 MIP 서버를 통해 IP 주소를 가입자 단말(20)에 제공하여 IP 결 설정을 수행한다(S80).

IP 주소를 부여받은 가입자 단말에게 본격적인 트래픽 서비스를 제공하기 위해 기지국(20)은 트래픽 암호화 키를 생성 및 분배하는 절차를 수행한 후(S90), 각각 대한 트래픽 연결 설정을 수행한다(S100).

도 5는 도 4에 도시된 기본 기능 협상 과정 및 가입자 단말 인증 과정을 수행하 위해 가입자 단말(10)과 기지국(20) 간의 MAC 연결 절차를 나타내는 흐름도이다.

도 5를 참조하면, 가입자 단말(10)과 기지국(20) 간에 레인징 절차(S10 ~ S40) 끝나면, 가입자 단말(10)에 대한 인증을 위해 인증 모드 협상 과정을 포함한 기본 능 협상(Subscriber Station Basic Capablity Negotiation, 이하 "SBC"라고 함) 절 (S50)가 수행된다.

먼저, 가입자 단말(10)은 기본 기능 협상, 특히 인증 모드 선택을 위한 협상을 해 기지국(20)으로 기본 기능 협상 요구 메시지(SBC-Request)를 송신한다(S51). 때, 기본 기능 협상 메시지에는 인증 모드를 선택할 수 있도록 지원 가능한 인증 드 관련 파라미터가 포함되어 전달되며, 이러한 파라미터를 포함한 기본 기능 협상 시지에 대해서는 추후 설명한다.

다음, 가입자 단말(10)에서 송신된 기본 기능 협상 요구 메시지를 수신한 기지 (20)은 가입자 단말(10)에 대한 인증을 위해 IEEE 802.16의 프라이버시 규격에 미

정의된 기본 기능 협상을 수행하는 동시에, 기본 기능 협상 메시지에 포함된 인증 드 협상 파라미터를 통해서 수행 가능한 인증 모드를 확인한 후 하나의 인증 모드 선택한다. 예를 들어, 가입자 단말(10)에 대해 IEEE 802.16 프라이버시 규격에 른 인증 모드와 상위 계층의 표준화된 인증 프로토콜인 EAP-TLS 또는 EAP-TTLS 프 토콜에 따른 인증 모드가 있는 경우에 이들 중에서 하나의 인증 모드가 선택될 수 다.

기지국(20)은 인증 모드를 포함한 기본 기능 협상 결과를 기본 기능 협상 응답 시지(SBC-Reply)를 통해 가입자 단말(10)로 전송한다(S52).

따라서, 가입자 단말(10)은 기지국(20)과의 협상에 의해 선택된 인증 모드에 따 인증 절차를 수행한다.

이와 같이, 기지국(20)이 기본 기능 협상 메시지를 가입자 단말(10)로 전송함으 써, 가입자 단말(10)과 기지국(20)에서의 기본 기능 협상 절차(S50)가 끝나게 다.

그 후, 가입자 단말(10)과 기지국(20)은 상기 단계(S50)에서 선택된 인증 모드 따라 가입자 단말(10)에 대한 인증을 수행하는 절차(S60)를 수행한다.

만약 상기 기본 기능 협상 절차(S50)에서 IEEE 802.16 프라이버시 규격에 따른 지털 인증서 기반의 인증 모드가 선택되었으면, 가입자 단말(10)과 기지국(20)은 5에 도시된 'A' 부분의 가입자 인증 절차를 수행한다. 이러한 가입자 인증 절차 가입자 단말(10)이 기지국(20)으로 MAC 메시지중 인증 메시지인 PKM(Public Key nager) 메시지를 통해 가입자 디지털 인증서(CA-Certificate)를 기지국(20)으로 전

하는 PKM-REQ/Authentication Information 메시지 송신 과정(S61). 가입자 단말
0)이 가입자 인증 정보를 PKM 메시지를 통해 기지국(20)으로 전송하는
M-REQ/Authorization Request 메시지 송신 과정(S62) 및 기지국(20)으로부터의 인
수행 결과를 PKM 메시지를 통해 가입자 단말(10)로 전송하는
M-RSP/Autohrization Reply 메시지 송신 과정(S63)을 통해 수행되는 것에 대해서는
미 IEEE 802.16의 프라이버시 규격에 의해 공지되어 있으므로 여기에서는 상세한
명을 생략하여도 본 기술분야의 당업자에 의해 쉽게 이해될 것이다.

한편, 상기 기본 기능 협상 절차(S50)에서 EAP-TLS나 EAP-TTLS 프로토콜과 같은
위 계층의 표준화된 인증 프로토콜에 따른 인증 모드가 선택되었으면, 가입자 단말
0)과 기지국(20)은 도 5에 도시된 'B' 부분의 가입자 인증 절차를 수행한다.

이러한 가입자 인증 절차는 종래의 IEEE 802.16의 프라이버시 규격에 따른 인증
위한 MAC 메시지 중 PKM 메시지 중에 EAP 프레임워크를 수용할 수 있는 메시지를
가하여 수행된다.

먼저, 가입자 단말(10)은 EAP 기반의 인증을 수행하기 위한 메시지를 PKM 메시
중의 하나인 가입자 인증 요청 메시지(PKM-REQ/EAP-transfer request)를 통해 가
자의 인증 정보를 기지국(20)으로 전송한다(S61'). 이 때 전송되는 가입자 인증
청 메시지는 추후 설명한다.

다음, 기지국(20)은 가입자 단말(10)로부터 전송된 가입자 인증 요청 메시지를
아서 인증 서버인 AAA 서버(40)를 통해 가입자 단말(10)에 대한 인증을 수행한 후
결과를 가입자 인증 응답 메시지(PKM-REQ/EAP-transfer reply)를 통해 가입자 단
(10)로 전송한다(S62').

기지국(20)으로부터 가입자 단말(10)로 전송된 가입자 인증 응답 메시지내에 포함된 인증 결과가 인증 성공한 것으로 확인되면, 가입자 단말(10)은 가입자 단말(10)과 트래픽 보안을 위한 암호화 키를 요청하는 기지국(20)으로 PKM 메시지 중의 하나인 키 요청 메시지(Key Request)를 전송하고(S64), 기지국(20)은 가입자 단말(10)로부터 송신된 키 요청 메시지의 모든 필드 값들을 바탕으로 하여 암호화 키 생성 메커니즘으로 해당 가입자 단말(10)에 할당할 암호화 키를 생성한 후 그 결과를 PKM 메시지 중의 하나인 키 응답 메시지(Key Reply)를 통해 가입자 단말(10)로 전송한다(S65).

이와 같이, 기지국(20)이 키 응답 메시지를 가입자 단말(10)로 전송함으로써, 가입자 단말(10)에 대한 인증 절차(S60)가 끝나게 된다.

도 6은 도 5에 도시된 기본 기능 협상 과정에서 사용되는 기본 기능 협상 요구 메시지(SBC-REQ)의 포맷을 나타낸 도면이다.

도 6을 참조하면, 기본 기능 협상 요구 메시지인 SBC-REQ는 Management Message Type값으로 26을 가지며, TLV(Type/Length/Value) Encoded Information 포맷으로 파라미터의 융통성을 가진다.

이러한 기본 기능 협상 요구 메시지에 포함될 수 있는 TLV에는 물리 계층의 대역폭(bandwidth) 능력에 대한 협상을 위한 Bandwidth Allocation support와 가입자 단말(10)의 인증을 위한 인증 모드 선택을 위한 Authorization Policy Support를 비롯하여 복조기(demodulator), 변조기(modulator), FFT(Fast Fourier Transform)기 등 관련된 협상을 위한 Physical Parameter Support, Physical Parameter Support 내

포함되면서, 물리층의 변조 및 복조와 관련한 협상 파라미터, FFT 크기 협상을 위 "파라미터 등을 포함한다.

도 7은 본 발명의 실시예에 따른 무선 휴대 인터넷 시스템에서의 가입자 단말 증 방법에서 EAP 기반으로 가입자 단말을 인증하기 위한 MAC 흐름도이다.

도 7을 참조하면, 먼저 상기 도 5를 참조하여 설명한 바와 같이 본 발명의 실시에 따라 가입자 단말(10)과 기지국(20) 간에 기본 기능 협상 요구/응답 메시지 BC-REQ/SBC-RSP)를 송수신하여 가입자 단말(10)과 기지국(20) 간에 인증 모드 협상 수행하는 절차가 진행된다(S100).

이러한 절차(S100)에 의해 가입자 단말(10)과 기지국(20) 간에 인증 모드 협상 이루어져서 가입자 단말(10)에 대한 인증 모드가 설정된다. 예를 들어, IEEE 2.16 프라이버시 규격에 따른 디지털 인증서 기반의 인증 모드와 EAP 기반의 상위 층의 표준화된 인증 프로토콜 기반의 인증 모드 중 어느 하나가 상기 협상에 의해 정된다.

IEEE 802.16 프라이버시 규격에 따른 디지털 인증서 기반의 인증에 대해서는 이 잘 알려져 있으므로 EAP 기반의 인증 모드로 선택된 경우에 대해 설명한다.

가입자 단말(10)은 MAC 메시지 중 인증 메시지인 PKM 메시지를 통하여 새롭게 가된 가입자 인증 요청 메시지(EAP-transfer request) 내에 EAP위에 올라가는 응용 층의 보안 프로토콜인 TLS 또는 TTLS 등의 데이터, 예를 들어 EAP 데이터 페이로드 ayload)를 실어 기지국(20)으로 전달하고(S110), 기지국(20)에서는 가입자 단말 0)로부터 수신된 MAC 메시지 중에서 인증 서버인 AAA 서버(40)로 보내질 데이터를

송하여 국제 표준화 기구(Internet Engineer Task Force: IETF)에서 표준화가 진행어 이미 잘 알려져 있는 다이아메터(Diameter) 프로토콜을 통해 AAA 서버(40)로 보다(S120).

AAA 서버(40)는 기지국(20)으로부터 전달되는 데이터를 처리하여 그 결과 메시를 다시 다이아메터 프로토콜을 통해 기지국(20)으로 전달하면(S130) 기지국(20)은 AA 서버(40)로부터 전달되는 결과 메시지를 받아서 PKM 메시지의 가입자 인증 응답 시지(EAP-transfer reply)를 통하여 가입자 단말(10)로 전달한다(S140).

이러한 가입자 단말(10)과 기지국(20) 간의 가입자 인증 요구/응답 메시지 AP-transfer request, EAP-transfer reply) 전달은 사용자 단말(10)에 대한 인증이 료될 때까지 반복된다. 이러한 반복 후에 인증 단계의 마지막 절차에서 가입자 단(10)이 전송한(S150) 가입자 인증 요구 메시지(EAP-transfer request)를 수신한 기국(20)이 AAA 서버(40)로 이 데이터를 전송하고(S160), AAA 서버(40)로부터 인증과를 받는다(S170).

만약 AAA 서버(40)로부터 해당 가입자에 대한 인증 결과가 성공이라는 메시지를으면 기지국(20)은 가입자 인증 응답 메시지(EAP-transfer reply)에 해당 가입자가용할 보안키를 생성하여 해당 키 관리를 위한 키 식별자(SAID), 라이프타임 ifetime) 등과 함께 가입자 단말(10)로 전달한 후(S180) 인증 절차를 종료한다.

그러나, AAA 서버(40)로부터 해당 가입자에 대한 인증 결과가 실패라는 메시지 받으면 기지국(20)은 가입자 인증 응답 메시지(EAP-transfer reply)에 인증 결과 나타내어 가입자 단말(10)로 전달한 후 인증 절차를 종료한다.

도 8은 본 발명의 실시예에 따른 무선 휴대 인터넷 시스템에서의 가입자 단말 증 방법에서 사용되는 MAC 메시지 중 PKM 메시지의 타입을 나타낸 도면이다.

도 8을 참조하면, 본 발명의 실시예에 따른 무선 휴대 인터넷 시스템에서의 가 자 단말 인증 방법에서는 MAC 메시지 중 PKM 메시지의 타입을 코드(code) 0에서부 14까지 정의하고 있다. 종래 IEEE 802.16 MAC 메시지 중 PKM 메시지에서는 10개 타입을 정의하고 있으며, 본 발명의 PKM 메시지 중 코드 3에서부터 12까지가 그것다. 즉, 본 발명의 실시예에서는 종래 IEEE 802.16에서의 PKM 메시지에 EAP 기반 상위 계층의 인증 프로토콜에 따른 인증 모드를 수행하기 위한 PKM 메시지 2개가 드 13과 14로써 추가된다. 이 때, 코드 13의 PKM 메시지는 PKM-REQ인 가입자 인증 구 메시지로 "EAP-transfer request"이고, 코드 14의 PKM 메시지는 PKM-RSP인 가입 인증 응답 메시지로 "EAP-transfer reply"이다.

따라서, 도 7에 도시된 인증 모드 협상 단계(S100)에서 IEEE 802.16 프라이버시 1반의 인증 모드로 설정된 경우에는 코드 4, 5, 6, 10 및 12 등의 PKM 메시지를 사 하여 가입자 단말(10)에 대한 인증이 수행되고, EAP 기반의 인증 모드로 설정된 경 에는 코드 13 및 14의 PKM 메시지를 사용하여 가입자 단말(10)에 대한 인증이 수행 다. 이 때, 코드 13의 가입자 인증 요구 메시지인 PKM 메시지는 가입자 단말(10) 서 기지국(20)으로 전달되는 PKM-REQ 메시지이고, 코드 14의 가입자 인증 응답 메 지인 PKM 메시지는 기지국(20)으로부터 가입자 단말(10)로 전달되는 PKM-RSP 메시 이다.

도 9는 도 8에 도시된 PKM 메시지 중에서 EAP 기반의 가입자 인증을 위한 메시 의 구성요소를 나타낸 도면이다.

도 9를 참조하면, EAP 기반의 가입자 인증을 위한 코드 13의 가입자 인증 요구 지지(EAP-transfer request)에는 가입자 단말(10)에서 기지국(20)으로 전송하는 메지로 Security-Capabilities, SAID 및 EAP 페이로드(Payload) 파라미터가 함된다.

Security-Capabilities는 가입자 단말(10)의 Securoty Capability를 기술할 수는 파라미터이다.

SAID는 가입자 단말(10)과 기지국(20)에서 보안 프로토콜을 운용하여 통신하고 할 때 선택가능한 Security Association을 구분할 수 있는 일련번호이다.

EAP 페이로드는 EAP 상위에 올라가는 사용자 인증을 위한 프로토콜용 데이터를 타낸다.

한편, EAP 기반의 가입자 인증을 위한 코드 14의 가입자 인증 응답 메시지 AP-transfer reply)에는 기지국(20)에서 가입자 단말(10)로 전송하는 메시지로 EAP sult Code, Authorization Action Code, Key Sequence Number, Key Life Time, SA criptor 및 EAP 페이로드가 포함된다.

EAP Result Code는 가입자 단말(10)로부터 전송된 EAP-transfer request에 대한 리 결과를 나타낸다.

Authorization Action Code는 인증 수행 결과 실패인 경우 가입자 단말(10)에서 할 수 있는 인증 절차(초기 인증, 재인증)를 제시한다.

Key Sequence Number와 Key Life Time은 인증이 성공한 경우 해당 가입자에게 배되는 키와 관련된 파라미터이다.

SA Descriptor는 가입자 단말(10)과 기지국(20)에서 수용할 수 있는 시큐리티 (security set)에 대한 설명을 나타낸다.

EAP 페이로드는 상위 보안 프로토콜용 데이터를 나타낸다.

이러한 가입자 인증 응답 메시지에 포함되는 파라미터들 중에서 인증 중간에 발 하는 가입자 인증 응답 메시지에는 키 관련 파라미터인 Key Sequence Number 및 y Life Time은 포함되지 않고, 인증 마지막 단계에서 인증 결과 성공인 경우에만 함된다.

도 10은 도 6에 도시된 기본 기능 협상 요구 메시지(SBC-REQ)의 파라미터 중 thorization Policy Support 파라미터의 속성을 나타낸 도면이다.

도 10을 참조하면, 가입자 단말(10)에 대한 인증 모드 협상을 위해 사용되는 thorization Policy Support 파라미터는 그 타입(Type)이 5.21이고, 길이(Length) 1바이트이며, 그 값(Value)은 비트맵(Bitmap) 방식으로 규정된다.

이러한 파라미터의 값(Value)에서, 비트 0은 IEEE 802.16에서 정의하고 있는 기 의 프라이버시 모드의 설정을 나타내고, 비트 1은 EAP 기반의 상위 계층의 인증 프 토콜에 따른 인증 모드의 설정을 나타낸다. 그 외의 비트는 현재 보류(reserved) 어 있으나, 비트 1이 설정되어 EAP 기반의 인증 모드가 설정된 경우, 보류되어 있 비트들, 즉 비트 2 내지 7을 사용하여 현재 제공하는 EAP 기반의 상위 인증 플랫 을 나타낸다. 구체적으로, 비트 2는 EAP-TLS 인증 프로토콜의 설정을 나타내고, 트 3은 EAP-TTLS 인증 프로토콜의 설정을 나타내며, 나머지 비트들에 대해서는 추 지원 가능한 응용 계층의 표준화 보안 프로토콜의 추가에 따라 확장 가능하다.

이하, 상기한 본 발명의 실시예에 따른 무선 휴대 인터넷 시스템에서 가입자 단의 인증을 수행하는 장치의 일예에 대해 설명한다.

도 11은 본 발명의 실시예에 따른 무선 휴대 인터넷 시스템에서의 가입자 단말 증 장치의 블록도이다.

도 11에 도시된 바와 같이, 본 발명의 실시예에 따른 무선 휴대 인터넷 시스템 서의 가입자 단말 인증 장치는 가입자 단말(100), 기지국(200) 및 AAA 서버(300)를 t함한다.

가입자 단말(100)은 단말기 제어 장치(110), 디지털 신호 송수신 장치(120) 및 날로그 신호 송수신 장치(130)를 포함한다.

단말기 제어 장치(110)는 인증 요청부(111)를 포함하고, 디지털 신호 송수신 장(120)는 디지털 신호의 송/수신 기능을 수행하는 송신부(121) 및 수신부(122)를 포한다. 여기서, 본 발명의 실시예에 따른 단말기 제어 장치(110)는 상기한 인증 요부(111) 이외에도 기지국(200)과의 데이터 송수신 및 데이터 처리를 위한 다수의 치를 더 포함할 수 있으며, 이러한 장치들은 이미 공지된 기술임으로 여기서는 상한 설명을 생략한다.

인증 요청부(111)는 가입자 단말(100)의 인증을 기지국(200)으로 요청하며, 기국(200)과의 협상에 의해 설정되는 인증 모드에 따라 기지국(200) 또는 AAA(300) 버와의 인증을 수행한다.

도 12는 도 11에 도시된 가입자 단말(100)의 인증 요청부(111)의 상세 블록도이

도 12에 도시된 바와 같이, 인증 요청부(111)는 인증 요청 메시지 생성부(111a), 인증 응답 메시지 분석부(111b), 메모리(111c) 및 인증 요청 제어부(111d)를 포함한다.

인증 요청 메시지 생성부(111a)는 기지국(200)에게 가입자 단말(100)에 대한 인증을 요청하는 인증 모드 협상 관련 메시지 및 가입자 인증 요청 메시지를 생성하여 디지털 신호 송수신 장치(120)로 전달한다. 이 때 생성되는 인증 모드 협상 관련 메시지는 MAC 메시지 중의 하나인 SBC-REQ 메시지로써 생성되며, 도 6 및 도 10에 도시된 바와 같이 종래의 IEEE 802.16에서의 SBC-REQ 메시지에 인증 모드 협상을 위한 "Authorization Policy Support" 파라미터가 포함된다. 또한, 가입자 인증 요청 메시지는 MAC 메시지 중의 하나인 PKM-REQ 메시지로써 생성되며, 도 8 및 도 9에 도시된 바와 같이 종래의 IEEE 802.16에서의 PKM-REQ 메시지에 EAP 기반의 상위 계층의 인증 프로토콜에 의한 인증이 AAA 서버(300)에 의해 수행될 수 있도록 하는 메시지이다.

인증 응답 메시지 분석부(11b)는 기지국(200)으로부터 MAC 메시지 중 하나인 C-RSP 메시지를 이용하여 송신되는 인증 모드 협상 관련 메시지 및 가입자 인증 응답 메시지를 디지털 신호 송수신 장치(120)를 통해 수신하여 분석하고, 그 분석 결과를 인증 요청 제어부(111d)로 전달한다. 인증 응답 메시지 분석부(111b)에 의해 분석되는 결과는 인증 모드 설정 여부와 인증 결과 등이다.

메모리(111c)는 인증 응답 메시지 분석부(111b)에 의해 분석된 결과를 저장한다. 예를 들어 협상되어 설정된 인증 모드나 인증 실패시 발생된 에러 등을 저장한다.

인증 요청 제어부(111d)는 기지국(200)에게 가입자 단말(100)에 대한 인증을 요하고, 기지국(200)으로부터의 응답을 받아서 처리하기 위해 인증 요청 메시지 생성(111a), 인증 응답 메시지 분석부(111b) 및 메모리(111c)의 동작을 제어한다.

다음, 디지털 송수신 장치(120)는 단말기 제어 장치(110)로부터 전달되는 신호 아날로그 신호 송수신 장치(130)를 통해 기지국(200)으로 송신하기 위한 송신부 21)와, 아날로그 신호 송수신 장치(130)를 통해 수신되는 신호를 수신하여 단말기 어 장치(110)로 전달하는 수신부(122)를 포함한다. 특히, 송신부(121)는 위에 기된 바와 같은 구조로 이루어지는 단말기 제어 장치(110)로부터 전달되는 인증 요청 ‖시지(SBC_REQ, PKM-REQ)를 변조 및 부호화하며, 아날로그 신호 송수신 장치(130) 이렇게 변조 및 부호화된 메시지를 안테나(140)를 통해 무선으로 기지국(200)으로 신한다.

또한, 아날로그 신호 송수신 장치(130) 및 디지털 송수신 장치(120)의 수신부 22)는 기지국(200)으로부터 무선으로 송신되어 안테나(140)를 통해 수신되는 인증 답 메시지(SBC-RSP, PKM-RSP)를 수신하여 단말기 제어 장치(110)로 전달한다.

한편, 기지국(200)은 기지국 제어 장치(210), 디지털 신호 송수신 장치(220, 0) 및 아날로그 신호 송수신 장치(240)를 포함한다.

기지국 제어 장치(210)는 가입자 단말(100)로부터의 가입자 인증 요청에 따라 증 모드를 설정하고 설정된 인증 모드에 따른 인증을 수행한다. 이 때, 인증 모드 IEEE 802.16 프라이버시 기반의 인증 모드이면 기지국(200)에서 인증이 이루어지만, 만약 인증 모드가 EAP 기반의 상위 계층의 인증 프로토콜에 따른 인증 모드이

기지국(200)은 AAA 서버(300)를 통해서 인증을 수행한다. 이를 위해서 기지국 제어 장치(210)는 인증 처리부(211)를 포함한다.

도 13은 도 11에 도시된 기지국(200)의 인증 처리부(211)의 상세 블록도이다.

도 13에 도시된 바와 같이, 인증 처리부(211)는 메시지 분석부(211a), 인증 응답 메시지 생성부(211b), 상위 인증 요청 메시지 생성부(211c), 메모리(211d) 및 인터페이스 제어부(211e)를 포함한다.

메시지 분석부(211a)는 디지털 신호 송수신 장치(220)를 통해 가입자 단말(100)로부터 수신되는 MAC 메시지 중 인증 모드 협상 메시지(SBC-REQ)와 가입자 인증 요청 메시지(PKM-REQ)를 분석하고, 또한 디지털 신호 송수신 장치(230)를 통해 AAA 서버(300)로부터 수신되는 상위 계층의 인증 프로토콜 관련 메시지인 다이아메터 메시지를 분석한 후, 그 분석 결과를 인증 제어부(211e)로 전달한다.

인증 응답 메시지 생성부(211b)는 가입자 단말(100)로부터의 인증 모드 협상 메시지 또는 가입자 인증 요청 메시지에 대한 응답 메시지를 생성하여 디지털 신호 송수신 장치(120)를 통해 가입자 단말(100)로 전달한다.

상위 인증 요청 메시지 생성부(211c)는 가입자 단말(100)과의 인증 모드 협상 과정에서 인증 모드가 EAP 기반의 상위 계층의 인증 모드로 설정된 경우에 AAA 서버(300)에게 가입자 단말(100)에 대한 인증을 요청하는 다이아메터 프로토콜 메시지를 생성하여 디지털 신호 송수신 장치(230)를 통해 AAA 서버(300)로 송신한다.

메모리(211d)는 메시지 분석부(211a)에 의해 분석된 결과를 저장한다. 예를 들어 협상되어 설정된 인증 모드나 인증 실패시 발생된 에러 등을 저장한다.

인증 제어부(211e)는 가입자 단말(100)로부터의 인증 요청에 따른 처리를 수행하여 응답하고, 인증 모드가 EAP 기반의 상위 계층의 인증 모드인 경우에는 AAA 서버(300)에게 가입자 단말(100)에 대한 인증을 요청하고, AAA 서버(300)로부터의 응답을 받아서 처리하기 위해 메시지 분석부(211a), 인증 응답 메시지 생성부(211b), 위 인증 요청 메시지 생성부(211c) 및 메모리(211d)의 동작을 제어한다.

다음, 디지털 송수신 장치(220)는 기지국 제어 장치(210)로부터 전달되는 신호를 아날로그 신호 송수신 장치(230)를 통해 가입자 단말(100)로 송신하기 위한 송신부(221)와, 아날로그 신호 송수신 장치(240)를 통해 수신되는 신호를 수신하여 기지국 제어 장치(210)로 전달하는 수신부(222)를 포함한다. 특히, 송신부(221)는 위에 설명된 바와 같은 구조로 이루어지는 기지국 제어 장치(210)로부터 전달되는 인증 응답 메시지(SBC_RSP, PKM-RSP)를 변조 및 부호화하며, 아날로그 신호 송수신 장치(240)는 이렇게 변조 및 부호화된 메시지를 안테나(250)를 통해 무선으로 가입자 단말(100)로 송신한다.

또한, 아날로그 신호 송수신 장치(240) 및 디지털 송수신 장치(220)의 수신부(222)는 가입자 단말(100)로부터 무선으로 송신되어 안테나(250)를 통해 수신되는 인증 요청 메시지(SBC-REQ, PKM-REQ)를 수신하여 기지국 제어 장치(210)로 전달한다.

다음, 디지털 송수신 장치(230)는 기지국 제어 장치(210)로부터 전달되는 신호를 AAA 서버(300)로 송신하기 위한 송신부(231)와, AAA 서버(300)로부터 수신되는 신호를 기지국 제어 장치(210)로 전달하는 수신부(232)를 포함한다. 이 때, 송수신부(231, 232)는 기지국 제어 장치(210)와 AAA 서버(300) 사이에 EAP 기반의 인증 프로토콜 관련 메시지, 예를 들어 다이아메터 메시지를 전달한다.

한편, AAA 서버(300)는 AAA 서버 제어 장치(310) 및 디지털 신호 송수신 장치(320)를 포함한다.

AAA 서버 제어 장치(310)는 기지국(200)으로부터의 EAP 기반의 상위 계층의 가입자 인증 요청에 따라 가입자 인증을 수행하며, 인증 처리부(311)를 포함한다.

도 14는 도 11에 도시된 AAA 서버(300)의 인증 처리부(311)의 상세 블록도이다.

도 14에 도시된 바와 같이, 인증 처리부(311)는 상위 인증 요청 메시지 분석부(311a), 상위 인증 응답 메시지 생성부(311b), 메모리(311c) 및 인증 제어부(311d)를 포함한다.

상위 인증 요청 메시지 분석부(311a)는 디지털 신호 송수신 장치(320)를 통해 기지국(200)으로부터 수신되는 상위 계층의 인증 프로토콜 메시지, 예를 들어 다이아미터 메시지를 분석하여 그 결과를 인증 제어부(311d)로 전달한다.

상위 인증 응답 메시지 생성부(311b)는 기지국(200)으로부터의 상위 인증 요청 메시지에 대한 응답 메시지를 생성하여 디지털 신호 송수신 장치(320)를 통해 기지국(200)으로 전달한다.

메모리(311c)는 메시지 분석부(311a)에 의해 분석된 결과를 저장한다. 예를 들어 인증 실패시 발생된 에러 등을 저장한다.

인증 제어부(311d)는 기지국(200)으로부터의 상위 계층의 인증 요청에 따른 처리를 수행하여 응답하기 위해 메시지 분석부(311a), 상위 인증 응답 메시지 생성부(311b) 및 메모리(311c)의 동작을 제어한다.

다음. 디지털 송수신 장치(320)는 AAA 서버 제어 장치(310)로부터 전달되는 신호를 기지국(200)으로 송신하기 위한 송신부(321)와, 기지국(200)으로부터 수신되는 호를 AAA 서버 제어 장치(310)로 전달하는 수신부(322)를 포함한다. 이 때, 송수부(321, 322)는 AAA 서버 제어 장치(310)와 기지국(200) 사이에 EAP 기반의 인증 로토콜 관련 메시지, 예를 들어 다이아메터 메시지를 전달한다.

이상에서 본 발명의 바람직한 실시예에 대하여 상세하게 설명하였지만 본 발명이에 한정되는 것은 아니며, 그 외의 다양한 변경이나 변형이 가능하다.

발명의 효과]

본 발명에 따르면, IEEE 802.16에서 지원하는 가입자 단말의 인증 기능에 이동 입자 단말에 대한 지원이 가능해진다.

또한, 서로 다른 사업자 망들간에 연동 또는 동일 사업자이지만 서로 다른 망으 구성된 경우에 대해서도 이들 망간의 연동 지원이 가능해진다.

또한, 표준화된 상위 계층의 보안 프로토콜을 지원하므로 확장성이 좋고, 안정면에서도 검증된 표준 보안 프로토콜을 사용하므로 월등히 유리하다.

【특허청구범위】

【청구항 1】

무선 휴대 인터넷 시스템에서 기지국에 무선 연결된 가입자 단말이 기지국으로 인증을 요청하는 방법에 있어서,

a) 인증 모드 설정을 위해 기본 능력 협상 메시지를 상기 기지국으로 송신하는 단계;

b) 상기 기지국에서 송신된 상기 기본 능력 협상 메시지에 대한 응답 메시지를 수신하여 인증 모드를 설정하는 단계; 및

c) 상기 설정된 인증 모드에 대응되는 가입자 인증 요청 메시지를 상기 기지국으로 송신하여 상기 가입자 단말에 대한 인증을 요청하는 단계

를 포함하는 무선 휴대 인터넷 시스템에서의 가입자 단말 인증 요청 방법.

【청구항 2】

제1항에 있어서,

상기 a) 단계에서,

상기 기본 능력 협상 메시지에는 인증 모드 설정이 가능한 파라미터가 포함된 것을 특징으로 하는 무선 휴대 인터넷 시스템에서의 가입자 단말 인증 요청 방법.

【청구항 3】

제2항에 있어서,

상기 기본 능력 협상 메시지는 IEEE 802.16 프라이버시(Privacy) 표준 프로토콜 MAC(Massage Authentication Code) 메시지 중의 하나인 SBC-REQ(Subscriber

ation Basic Capablity Negotiation - Request) 메시지에 인증 모드 설정이 가능한 파라미터가 포함된 메시지인 것을 특징으로 하는 무선 휴대 인터넷 시스템에서의 가입자 단말 인증 요청 방법.

【청구항 4】

제1항에 있어서,

상기 b) 단계에서,

상기 인증 모드는 IEEE 802.16 프라이버시 표준 프로토콜에 기반한 인증 모드와 상위 계층의 표준화된 인증 프로토콜에 기반한 인증 모드 중 어느 하나인 것을 특징으로 하는 무선 휴대 인터넷 시스템에서의 가입자 단말 인증 요청 방법.

【청구항 5】

제4항에 있어서,

상기 b) 단계에서 상기 인증 모드가 IEEE 802.16 프라이버시 표준 프로토콜에 기반한 인증 모드로 설정된 경우,

상기 c) 단계에서, 상기 기지국에 의한 가입자 인증을 요청하는 가입자 인증 요청 메시지를 상기 기지국으로 송신하는

것을 특징으로 하는 무선 휴대 인터넷 시스템에서의 가입자 단말 인증 요청 방법.

【청구항 6】

제5항에 있어서,

상기 기지국에 의한 가입자 인증을 요청하는 가입자 인증 요청 메시지는 상기 IEEE 802.16 프라이버시 표준 프로토콜의 MAC 프로토콜 데이터인 PKM-REQ(Public Key Manager - Request) 메시지 중 Auth Info 메시지 및 Auth Request 메시지인 것을 특징으로 하는 무선 휴대 인터넷 시스템에서의 가입자 단말 인증 요청 방법.

【청구항 7】

제4항에 있어서,

상기 b) 단계에서 상기 인증 모드가 상위 계층의 표준화된 인증 프로토콜에 기반한 인증 모드로 설정된 경우,

상기 c) 단계에서, 상기 기지국에 접속되어 상기 가입자에 대한 인증을 수행하는 인증 서버(AAA:Authentication Authorization and Accounting 서버)에 의한 가입자 인증을 요청하는 가입자 인증 요청 메시지를 상기 기지국을 통해 상기 인증 서버로 송신하는

것을 특징으로 하는 무선 휴대 인터넷 시스템에서의 가입자 단말 인증 요청 방법.

【청구항 8】

제7항에 있어서,

상기 인증 서버에 의한 가입자 인증을 요청하는 가입자 인증 요청 메시지는 상기 IEEE 802.16 프라이버시 표준 프로토콜의 MAC 프로토콜 데이터인 PKM-REQ(Public Key Manager - Request) 메시지에 추가되어 상위 계층의 표준화된 인증 프로토콜에

반한 가입자 인증을 기지국에게 요청하는 것을 특징으로 하는 무선 휴대 인터넷 시템에서의 가입자 단말 인증 요청 방법.

【구항 9】

제4항 내지 제8항 중 어느 한 항에 있어서,

상기 상위 계층의 표준화된 인증 프로토콜은 EAP-TLS(Extensible thentication Protocol-Transport Layer Security) 및 EAP-TTLS(EAP-Tunneled TLS) 어느 하나인 것을 특징으로 하는 무선 휴대 인터넷 시스템에서의 가입자 단말 인 요청 방법.

【구항 10】

무선 휴대 인터넷 시스템에서 기지국에 무선 연결된 가입자 단말에 대한 인증을 행하는 방법에 있어서,

a) 상기 가입자 단말로부터 수신되는 인증 모드 설정을 위한 기본 능력 협상 시지에 따라 인증 모드를 설정한 응답 메시지를 상기 가입자 단말로 송신하는 단계

b) 상기 가입자 단말로부터 가입자 인증을 요청하는 메시지를 수신하여 직접 인을 수행하거나 또는 상기 기지국에 접속되어 상기 가입자에 대한 인증을 수행하는 증 서버(AAA:Authentication Authorization and Accounting 서버)에게 가입자 인증 요청하는 단계: 및

c) 상기 인증 결과를 나타내는 응답 메시지를 상기 가입자 단말로 송신하는 단

를 포함하는 무선 휴대 인터넷 시스템에서의 가입자 단말 인증 방법.

청구항 11]

제10항에 있어서,

상기 a) 단계에서,

상기 인증 모드는 IEEE 802.16 프라이버시 표준 프로토콜에 기반한 인증 모드와 상위 계층의 표준화된 인증 프로토콜에 기반한 인증 모드 중 어느 하나인 것을 특징으로 하는 무선 휴대 인터넷 시스템에서의 가입자 단말 인증 방법.

청구항 12]

제11항에 있어서,

상기 a) 단계에서 상기 설정된 인증 모드가 상기 상위 계층의 표준화된 인증 로토콜에 기반한 인증 모드인 경우,

상기 b) 단계에서 상기 인증 서버에게 상위 계층의 표준화된 인증 프로토콜을 해 상기 가입자에 대한 인증을 요청하는

것을 특징으로 하는 무선 휴대 인터넷 시스템에서의 가입자 단말 인증 방법.

청구항 13]

제12항에 있어서,

상기 상위 계층의 표준화된 인증 프로토콜은 다이아메터 프로토콜(Diameter otocol)인 것을 특징으로 하는 무선 휴대 인터넷 시스템에서의 가입자 단말 인증 법.

청구항 14】

제10항에 있어서,

상기 b) 단계에서 상기 기지국에 의해 가입자 인증이 수행되는 경우,

상기 c) 단계에서 상기 인증 결과를 나타내는 응답 메시지는 상기 IEEE 802.16 라이버시 표준 프로토콜의 MAC 프로토콜 데이터인 PKM-RSP(Public Key Manager - ply) 메시지 중 Auth Reply 메시지인 것을 특징으로 하는 무선 휴대 인터넷 시스템 서의 가입자 단말 인증 방법.

청구항 15】

제10항에 있어서,

상기 b) 단계에서 상기 인증 서버에 의해 상위 계층의 표준화된 인증 프로토콜 기반한 가입자 인증이 수행되는 경우,

상기 c) 단계에서 상기 인증 결과를 나타내는 응답 메시지는 상기 IEEE 802.16 라이버시 표준 프로토콜의 MAC 프로토콜 데이터인 PKM-RSP(Public Key Manager - ply) 메시지에 추가되어 상위 계층의 표준화된 인증 프로토콜에 기반한 가입자 인 결과를 상기 가입자 단말로 송신하는 것을 특징으로 하는 무선 휴대 인터넷 시스 에서의 가입자 단말 인증 방법.

청구항 16】

무선 휴대 인터넷 시스템에서 가입자 단말과 기지국 간에 가입자 단말에 대한 증을 수행하는 프로토콜을 구성하는 방법에 있어서,

a) 상기 가입자 단말과 기지국 간에 인증 모드 설정을 위한 기본 능력 협상 메지를 MAC 메시지를 이용하여 송수신하는 단계; 및

b) 상기 가입자 단말과 기지국 간에 상기 a) 단계에서 설정된 인증 모드에 따른 입자 인증 메시지를 MAC 메시지를 이용하여 송수신하는 단계

를 포함하는 무선 휴대 인터넷 시스템에서의 가입자 단말 인증 프로토콜 구성 법.

청구항 17】

제16항에 있어서,

상기 a) 단계에서,

상기 기본 능력 협상 메시지는 IEEE 802.16 프라이버시 표준 프로토콜의 MAC 메지 중 하나인 SBC-REQ 및 SBC-RSP 메시지에 인증 모드 설정이 가능한 파라미터가 함된 메시지를 이용하여 전송되는 것을 특징으로 하는 무선 휴대 인터넷 시스템에의 가입자 단말 인증 프로토콜 구성 방법.

청구항 18】

제16항에 있어서,

상기 b) 단계에서,

상기 가입자 인증 메시지는 IEEE 802.16 표준 프로토콜의 MAC 메시지 중 하나인 PKM-REQ 및 PKM-RSP 메시지 또는 상기 PKM-REQ 및 PKM-RSP 메시지에 상위 계층의 표준화된 프로토콜에 따른 인증을 수행하기 위한 메시지를 이용하여 전송되는 것을 특징으로 하는 무선 휴대 인터넷 시스템에서의 가입자 단말 인증 프로토콜 구성 방법.

【청구항 19】

제18항에 있어서,

상기 상위 계층의 표준화된 프로토콜에 따른 인증을 수행하기 위한 메시지는 상기 상위 계층의 표준화된 프로토콜이 EAP 기반의 프로토콜인 경우,

상기 가입자 단말로부터 상기 기지국으로 송신되는 메시지는 PKM-REQ/EAP-transfer request이고,

상기 기지국으로부터 상기 가입자 단말로 송신되는 메시지는 PKM-REQ/EAT-transfer reply인

것을 특징으로 하는 무선 휴대 인터넷 시스템에서의 가입자 단말 인증 프로토콜 구성 방법.

【청구항 20】

무선 휴대 인터넷 시스템에서 기지국에게 인증을 요청하는 가입자 단말에 있어서,

상기 기지국에게 가입자 단말에 대해 수행될 인증 모드 설정을 요청하고, 상기 기지국에 의해 설정된 인증 모드에 따른 가입자 단말에 대한 인증을 상기 기지국으로 요청하는 단말기 제어 장치:

상기 단말기 제어 장치로 입출력되는 신호에 대한 변복조 및 채널 부호화를 수하는 디지털 신호 송수신 장치: 및

상기 디지털 신호 송수신 장치와 상기 기지국 간의 아날로그 무선 신호 전송을 개하는 아날로그 신호 송수신 장치

를 포함하는 가입자 단말.

【구항 21】

제20항에 있어서,。

상기 단말기 제어 장치는,

상기 기지국에게 상기 가입자 단말에 대한 인증을 요청하는 인증 모드 협상 관 메시지 및 가입자 인증 요청 메시지를 생성하여 상기 디지털 신호 송수신 장치를 해 상기 기지국으로 송신하는 인증 요청 메시지 생성부:

상기 기지국으로부터 송신되는 인증 모드 협상 관련 메시지 및 가입자 인증 응 메시지를 상기 디지털 신호 송수신 장치를 통해 수신하여 분석하는 인증 응답 메 지 분석부: 및

상기 기지국에게 상기 가입자 단말에 대한 인증을 요청하고, 상기 기지국으로부 의 응답을 받아서 처리하기 위해 상기 인증 요청 메시지 생성부 및 인증 응답 메시 분석부의 동작을 제어하는 인증 요청 제어부

를 포함하는 가입자 단말.

【청구항 22】

제20항 또는 제21항에 있어서,

상기 설정된 인증 모드에는 상위 계층의 표준화된 인증 프로토콜 기반의 인증 드가 포함되는 것을 특징으로 하는 가입자 단말.

【청구항 23】

무선 휴대 인터넷 시스템에서 가입자 단말에 대한 인증을 수행하는 기지국 장치 있어서,

상기 가입자 단말로부터의 인증 요청에 따라 인증 모드를 설정하고, 상기 설정 인증 모드에 따른 인증을 수행하는 기지국 제어 장치;

상기 기지국 제어 장치로 입출력되는 신호에 대한 변복조 및 채널 부호화를 수 하는 디지털 신호 송수신 장치; 및

상기 디지털 신호 송수신 장치와 상기 가입자 단말 간의 아날로그 무선 신호 전을 중개하는 아날로그 신호 송수신 장치

를 포함하는 기지국 장치.

【청구항 24】

제23항에 있어서,

상기 기지국 제어 장치는,

상기 디지털 신호 송수신 장치를 통해 상기 가입자 단말로부터 수신되는 인증 드 협상 및 가입자 단말 인증 관련 메시지를 분석하고, 또한 상기 가입자 단말에

한 상위 계층의 표준화된 인증 프로토콜 기반의 인증을 수행하는 인증 서버로부터 전송되는 상위 계층의 인증 프로토콜 관련 메시지를 분석하는 메시지 분석부;

상기 가입자 단말로부터의 인증 모드 협상 메시지 또는 가입자 인증 요청 메시지에 대한 응답 메시지를 생성하여 상기 디지털 신호 송수신 장치를 통해 상기 가입자 단말로 전달하는 인증 응답 메시지 생성부;

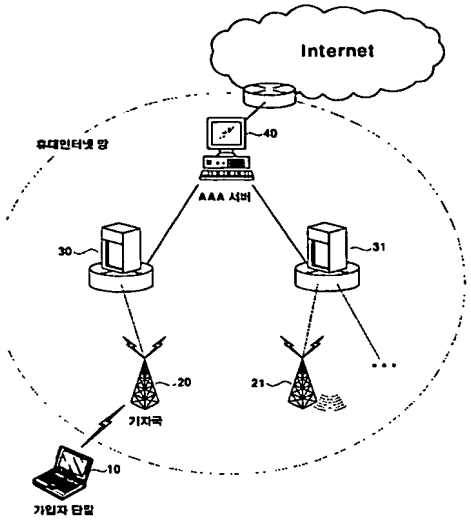
상기 가입자 단말과의 인증 모드 협상 과정에서 인증 모드가 상위 계층의 표준화된 인증 프로토콜 기반의 인증 모드로 설정된 경우에 상기 인증 서버에게 상기 가입자 단말에 대한 인증을 요청하는 메시지를 생성하여 상기 디지털 신호 송수신 장치를 통해 상기 인증 서버로 송신하는 상위 인증 요청 메시지 생성부; 및

상기 가입자 단말로부터의 인증 요청에 따른 처리를 수행하여 응답하고, 상기 인증 모드가 상위 계층의 인증 모드인 경우 상기 인증 서버에게 상기 가입자 단말에 대한 인증을 요청하고, 상기 인증 서버로부터의 응답을 받아서 처리하기 위해 상기 메시지 분석부, 인증 응답 메시지 생성부 및 상위 인증 요청 메시지 생성부의 동작을 제어하는 인증 제어부

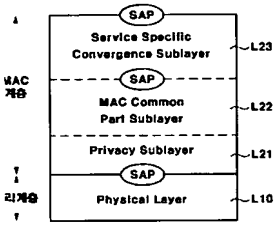
를 포함하는 기지국 장치.

【도면】

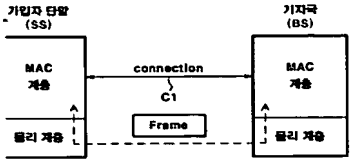
【도 1】


Internet
40
AAA 서버
30
31
20
21
기지국
10
가입자 단말

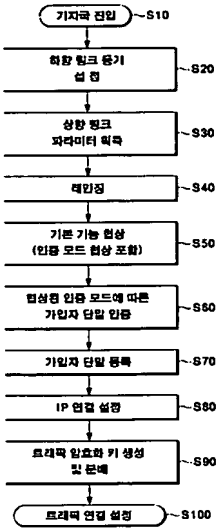
【도 2】


SAP
Service Specific Convergence Sublayer
L23
SAP
MAC Common Part Sublayer
L22
Privacy Sublayer
L21
SAP
Physical Layer
L10

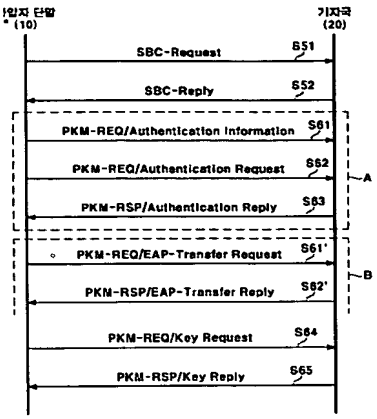
[도 3]


가입자 단말
(SS)
기지국
(BS)
MAC
계층
connection
C1
MAC
계층
Frame
물리 계층
물리 계층

[도 4]


기지국 진입
S10
하향 링크 동기
설 정
S20
상향 링크
파라미터 획득
S30
레인징
S40
기본 기능 협상
(인증 모드 협상 포함)
S50
협상된 인증 모드에 따른
가입자 단말 인증
S60
가입자 단말 등록
S70
IP 연결 설정
S80
트래픽 암호화 키 생성
및 분배
S90
트래픽 연결 설정
S100

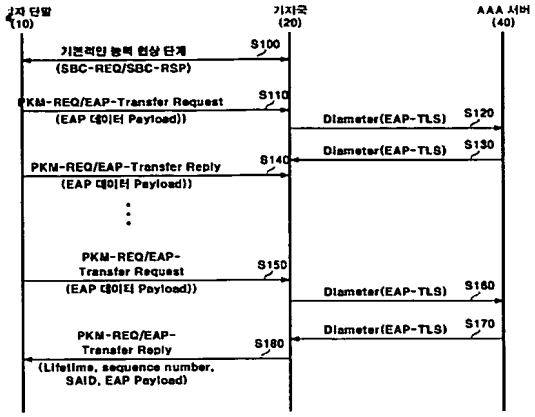
도 5]


가입자 단말
(10)
기지국
(20)
SBC-Request
S51
SBC-Reply
S52
PKM-REQ/Authentication Information
S61
PKM-REQ/Authentication Request
S62
A
PKM-RSP/Authentication Reply
S63
PKM-REQ/EAP-Transfer Request
S61'
B
PKM-RSP/EAP-Transfer Reply
S62'
PKM-REQ/Key Request
S64
PKM-RSP/Key Reply
S65

[표 6]

Syntax	Size	Notes
SBC-REQ_Message_Format() {		
Management Message Type = 28	8 bits	
TLV Encoded Information {	Variable	TLV specific
Bandwidth Allocation Support	8 bits	Bitmap 방식으로 지정
Authorization Policy Support	8 bits	Bitmap 방식으로 지정
Physical Parameters Supported {		
Demodulator	8 bits	Bit#0 = 64-QAM Support
Modulator	8 bits	Bit#0 = 64-QAM Support
FFT Size	8 bits	Bit#1 = FFT-2048
}		
}		
}		

도 7]


가입자 단말
(10)
기지국
(20)
AAA 서버
(40)
S100
기본적인 등록 협상 단계
(SBC-REQ/SBC-RSP)
S110
PKM-REQ/EAP-Transfer Request
(EAP 데이터 Payload))
Diameter(EAP-TLS)
S120
Diameter(EAP-TLS)
S130
S140
PKM-REQ/EAP-Transfer Reply
(EAP 데이터 Payload))
S150
PKM-REQ/EAP-
Transfer Request
(EAP 데이터 Payload))
Diameter(EAP-TLS)
S160
Diameter(EAP-TLS)
S170
S180
PKM-REQ/EAP-
Transfer Reply
(Lifetime, sequence number,
SAID, EAP Payload)

Ε 8]

Code	PKM Message Type	MAC Message Type
0~2	Reserved	
3	SA Add	PKM-RSP
4	Auth Request	PKM-REQ
5	Auth Reply	PKM-RSP
6	Auth Reject	PKM-RSP
7	Key Request	PKM-REQ
8	Key Reply	PKM-RSP
9	Key Reject	PKM-RSP
10	Auth Invalid	PKM-RSP
11	TEK Invalid	PKM-RSP
12	Auth Info	PKM-REQ
13	EAP-transfer Request	PKM-REQ
14	EAP-transfer Reply	PKM-RSP
15~255	reserved	

Ε 9]

AP transfer Request attributes

Attributes	Contents
Security-Capabilities	Describes requesting SS's security capabilities
SAID	SecurityAssociation ID, being equal to the Basic CID
EAP Payload	Contains the EAP-TLS Data, not interpreted in the MAC

AP transfer Reply attributes

Attributes	Contents
EAP Result Code	Describes success or failure
Authorization Action Code	Describes SS's policy, re-authorization or re-initialization
Key Sequence Number	Authorization Key sequence number
Key Life Time	Authorization Key life time
SA Descriptor	Specifies an SAID and additional properties of the SA
EAP Payload	Contains the EAP-TLS Data, not interpreted in the MAC

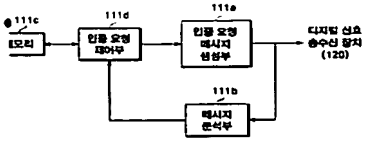
E 10]

Type	Length	Value	Scope
5.21	1	bit #0 : 802.16 Privacy - 701 bit # 1 : Open Privacy - 702 bit #2-7 : reserved; shall be set to zero - 703 (bit #2 : EAP-TLS, bit #3 : EAP-TTLS) - 704	SBC-REQ (see 1.1.1.1.1) SBC-RSP (see 1.1.1.1.2)

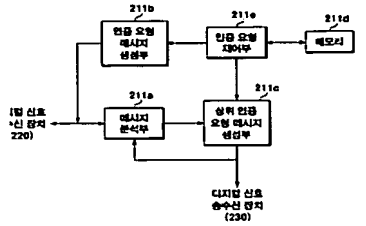
[도 11]

100
110
111
120
121
122
130
140
200
210
211
220
221
222
230
231
232
240
250
300
310
311
320
321
322
AAA 서버

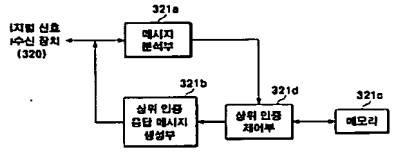
도 12]


111c
메모리
111d
인증 요청 제어부
111a
인증 요청 메시지 생성부
디지털 신호 송수신 장치 (120)
111b
메시지 분석부

도 13]


211b
인증 요청 메시지 생성부
211c
인증 요청 제어부
211d
메모리
211a
메시지 분석부
211c
상위 인증 요청 메시지 생성부
디지털 신호 송수신 장치 (230)

도 14]


321a
메시지 분석부
321b
상위 인증 응답 메시지 생성부
321d
상위 인증 제어부
321c
메모리

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/KR04/002766

International filing date: 29 October 2004 (29.10.2004)

Document type: Certified copy of priority document

Document details: Country/Office: KR
Number: 10-2004-0067733
Filing date: 27 August 2004 (27.08.2004)

Date of receipt at the International Bureau: 12 November 2004 (12.11.2004)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse